(10)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-037750
(43)Date of publication of application : 10.02.1994

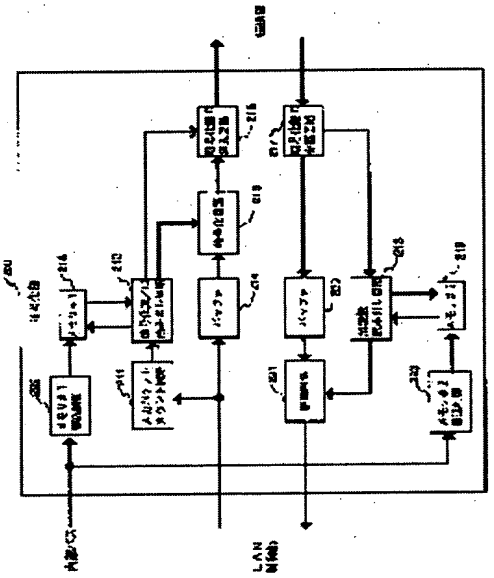
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04L 12/28

(21)Application number : 04-191893
(22)Date of filing : 20.07.1992

(71)Applicant : HITACHI LTD
(72)Inventor : ONO MASAFUMI
TAKIYASU YOSHIHIRO
ISHIDO TOMOAKI
SUZUKI HIDEYA

(54) INFORMATION TRANSFER SYSTEM

(57)Abstract:
PURPOSE: To decode ciphered information accurately even in ciphering communication using plural ciphering keys by transferring an identification number representing definitely a ciphered key/-decoding key together with ciphered information.
CONSTITUTION: An input packet count circuit 211 in a ciphering section 200 counts number of packets inputted from a LAN control section and transfers a count to a ciphering key/ID read circuit 212. Then the ciphering key/ID read circuit 212 reads a ciphering key identifier definitely representing the ciphering key used for ciphering a packet from a memory 213. That is, a means transferring the ciphering key together with ciphering information informs the ciphering key attended with the ciphering information to a reception terminal equipment. Then a means deciding a decoding key from the ciphering key in the received information in the reception terminal equipment decides a decoding key corresponding to the ciphering key used by the transmission terminal equipment.



LEGAL STATUS

[Date of request for examination] 09.04.1999
[Date of sending the examiner's decision of rejection] 22.04.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平6－37750

(43)公開日　平成６年(1994)２月10日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/06						
	9/14						
Ｇ０９Ｃ	1/00		9194－5L				
			7117－5K	Ｈ０４Ｌ	9／02	Ｚ	
			8529－5K		11／00	３１０　Ｚ	

審査請求　未請求　請求項の数32(全 27 頁)　最終頁に続く

(21)出願番号　特願平4－191893

(22)出願日　平成４年(1992)７月20日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大野　雅史
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　滝安　美弘
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　石藤　智昭
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

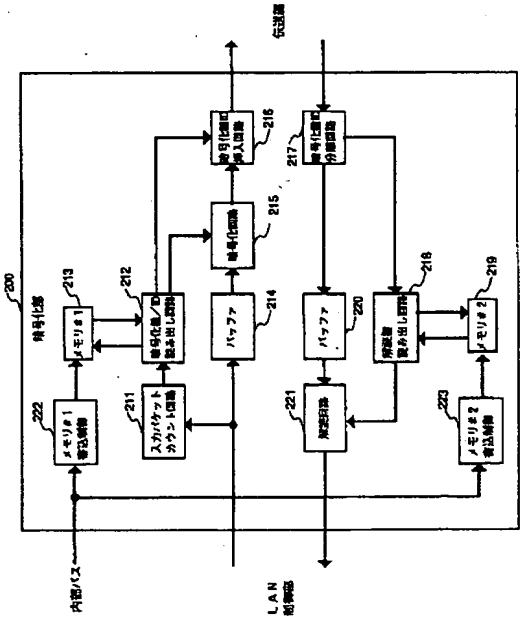
(54)【発明の名称】　情報転送方式

(57)【要約】

【構成】暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【効果】暗号化情報と共に暗号化鍵／解読鍵を一意に示す情報を転送するすることで、複数の暗号化鍵を用いる秘匿通信においても受信端末に暗号化鍵／解読鍵の識別情報を随時通知することが可能になるので、暗号化情報を正確に解読することができる。

図１



1

【特許請求の範囲】

【請求項1】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項2】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項3】請求項1または2において、ネットワーク内の全ての通信端末が解読可能な前記暗号化鍵を用いて、少なくとも暗号化鍵を暗号化する情報転送方式。

【請求項4】請求項1または2において、少なくとも暗号化鍵は暗号化せずに転送する情報転送方式。

【請求項5】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵に対応する解読鍵を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項6】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵に対応する解読鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項7】請求項5または6において、共通鍵を用いて、少なくとも前記解読鍵を暗号化する情報転送方式。

【請求項8】請求項5または6において、少なくとも前記解読鍵は暗号化せずに転送する情報転送方式。

【請求項9】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記暗号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項10】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗

2

号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵の識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項11】請求項9または10において、前記暗号化鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記暗号化鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項12】請求項9，10または11において、前記共通鍵を用いて、少なくとも前記暗号化鍵識別子を暗号化する情報転送方式。

【請求項13】請求項9，10または11において、少なくとも前記暗号化鍵識別子は暗号化せずに転送する情報転送方式。

【請求項14】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記解読鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項15】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記解読鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項16】請求項14または15において、前記解読鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記解読鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項17】請求項14，15または16において、前記共通鍵を用いて、少なくとも前記解読鍵識別子を暗号化する情報転送方式。

【請求項18】請求項14，15または16において、少なくとも前記解読鍵識別子は暗号化せずに転送する情報転送方式。

【請求項19】送信端末から受信端末に情報を暗号化し、暗号化情報をパケット化して転送する情報転送方式において、前記送信端末は2種類以上の暗号化鍵を用いて情報を暗号化し、パケットを組み立て、前記受信端末に転送することを特徴とする情報転送方式。

【請求項20】請求項19において、前記送信端末は使用する前記暗号化鍵を一意に示す前記暗号化鍵識別子を

3

決定する手段を具備し、前記暗号化情報を転送する毎に前記暗号化鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読する情報転送方式。

【請求項２１】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定することを特徴とする情報転送方式。

【請求項２２】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２３】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２４】請求項２１において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項２５】請求項２１，２２，２３または２４において、前記送信端末は、少なくとも前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を暗号化せずに、前記転送情報と共に転送する情報転送方式。

【請求項２６】請求項２１，２２，２３または２４において、前記送信端末は、前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を共通鍵を用いて暗号化して、前記転送情報と共に転送する情報転送方式。

【請求項２７】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は、前記送信端末から前記受信端末への転送経路を示すルート情報から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記ルート情報から解読鍵を決定することを特徴とする情報転送方式。

【請求項２８】請求項２７において、前記暗号化鍵を決定する手段として、一つあるいは複数のルート情報と一つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記ルート情報と一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

4

【請求項２９】請求項２７または２８において、前記送信端末は少なくとも前記ルート情報を暗号化せずに前記転送情報と共に転送する情報転送方式。

【請求項３０】請求項２７または２８において、前記送信端末は少なくとも前記ルート情報を前記共通鍵を用いて暗号化して前記転送情報と共に転送する情報転送方式。

【請求項３１】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング，リード・オンリー・メモリからのローディング，通信端末あるいは制御端末からのコマンド入力の内、少なくとも一つの手段により暗号化鍵を設定することを特徴とする情報伝送方式。

【請求項３２】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング，リードオンリーメモリからのローディング，通信端末あるいは制御端末からのコマンド入力の内、任意の複数の設定手段を有し、更に任意の設定手段を選択することを特徴とする情報転送方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、送信側通信端末（以下、送信端末と称す）から受信側通信端末（以下、受信端末と称す）に情報を暗号化して転送する情報転送方式に係り、特に、転送情報の送信先によって異なる暗号化アルゴリズム（以下、暗号化鍵と称す）を用いて情報を暗号化し転送する情報転送方式に関する。

【０００２】

【従来の技術】暗号を用いた従来の秘匿通信方式として、特開平3－262227 号公報に開示の技術がある。

【０００３】上記従来技術では、二つの通信局間で秘匿通信を行うために、双方の通信局に多数の暗証コードおよび暗号コード（暗号化鍵）を同じアドレスに記憶した暗証／暗号メモリを具備する。送信局は受信局に対して暗証／暗号メモリのアドレスを指定した応答要求信号を送信し、受信局は指定されたアドレスに記憶された暗証コードを読み出して、暗証コードを応答信号にのせて送信局に返信する。送信局は応答信号の暗証コードが正しいことを確認した後に、同アドレスの暗号コードを読み出し、暗号コードを用いて情報を暗号化した後に受信局に送信する。一方、受信局はアドレスの暗号コードを読み出し、暗号コードを用いて受信情報の解読を行う。

【０００４】

【発明が解決しようとする課題】上記従来技術をローカルエリアネットワーク（以下、ＬＡＮと称す）の様なコネクションレス通信（以下、ＣＬ通信と称す）に適用す

5

る場合には次のような問題点が生じる。

【０００５】先ず、ＣＬ通信には明確な通信の開始が無いので、秘匿通信に先立って暗号コードを転送することが出来ないという問題点がある。これに対して単一の暗号コードを使用するという方式が考えられるが、単一暗号コードを使用した場合は暗号コードを第三者が獲得しネットワーク内の情報を無断で入手する危険性が高くなるので好ましくない。

【０００６】ネットワークのセキュリティを向上させるには複数の暗号コードを用いれば良いが、ＣＬ通信では前述の様に通信に先立って暗号コードを通知することが出来ないので、次のような新たな問題点が発生する。すなわち、ＣＬ通信ではネットワーク内の各端末が受信するのは必ずしも自分宛の情報とは限らない。即ち、各端末はネットワーク上の転送情報を監視し、転送情報（パケット）に含まれるルート情報に基づきパケットが自分宛か否かを判断しパケットの取捨選択を行う。ここで、ネットワーク内で複数の異なる暗号化コードを用いて複数の異なるルート情報を暗号化した場合、異なるルート情報から同一の暗号化ルート情報が生成することが考えられる。即ち、このような場合には送受信端末間で暗号コードを一致させておかないと、本来受信しない情報を誤って受信してしまうことになる。

【０００７】従来技術の類似技術として、ＣＬ通信の任意の時点（例えば、始業時間）に暗号コードを通知するようにして、更に、異なるルート情報からは異なる暗号化ルート情報しか生成しないようにしても次のような問題点が生じる。すなわち、前述の様に、ＣＬ通信ではネットワーク上のパケットの取捨選択によりパケットを受信するか否かを決定するので、受信端末はパケット受信毎に全ての暗号コードを用いてパケットを解読しなくてはならない。これはネットワークのスループットの低下の原因になるばかりでなく、ハード量の増加の原因にもなる。

【０００８】本発明の目的は、送受信端末間の情報授受の機密性を維持するために複数の暗号化コード（暗号化鍵）を用いる情報転送方式において、暗号化情報の誤受信とこれに伴うスループットの低下、およびハード量の増加を防ぐ情報転送方式を提供することにある。

【０００９】

【課題を解決するための手段】前記課題を解決する第一の手段として、暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【００１０】前記課題を解決する第二の手段として、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵を読み出す手段を受信端末に設ける。

【００１１】前記課題を解決する第三の手段として、使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する

6

手段と、前記暗号化鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を受信端末に設ける。

【００１２】前記課題を解決する第四の手段として、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、前記解読鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵識別子から解読鍵を決定する手段を受信端末に設ける。

【００１３】前記課題を解決する第五の手段として、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段を受信端末に設ける。

【００１４】前記課題を解決する第六の手段として、ルート情報から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中のルート情報から解読鍵を決定する手段を受信端末に設ける。

【００１５】

【作用】第一の解決手段を用いた情報転送方式では、暗号化鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に暗号化鍵を通知することが可能になる。更に、受信した情報の中の暗号化鍵から解読鍵を決定する手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と暗号化鍵が対になって転送され、更に暗号化鍵から解読鍵を決定することが出来るので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１６】第二の解決手段を用いた情報転送方式では、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に解読鍵を通知することが可能になる。更に、受信した情報の中の解読鍵を読み出す手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と対応する解読鍵が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１７】第三の解決手段を用いた情報転送方式では、使用する暗号化鍵を一意に示す暗号化鍵識別子を暗号化情報と共に転送する手段により、受信端末に暗号化鍵識別子を通知することが可能になる。更に、暗号化鍵識別子から解読鍵を決定する手段により、暗号化鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と暗号化鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１８】第四の解決手段を用いた情報転送方式で

7

は、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を暗号化情報と共に転送する手段により、受信端末に解読鍵識別子を通知することが可能になる。更に、解読鍵識別子から解読鍵を決定する手段により、解読鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と解読鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【００１９】第五の解決手段を用いた情報転送方式では、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段と、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段により、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方のアドレスに対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では送信端末アドレスと受信端末アドレスを暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【００２０】第六の解決手段を用いた情報転送方式では、ルート情報から暗号化鍵を決定する手段と、受信した情報の中のルート情報から解読鍵を決定する手段により、ルート情報に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式ではルート情報を暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【００２１】

【実施例】図２は本発明を用いたＬＡＮ接続ボード１４０（以下、ＬＡＮインタフェースと称す）を装着したワークステーション（以下、ＷＳと称す）本体１００のブロック図である。

【００２２】図２において、ユーザＩ／Ｏインタフェース１１０，ＣＰＵ１２０，メモリ１３０，ＬＡＮインタフェース１４０，ＦＤ制御部１５０が内部バス１６０で接続されている。ユーザＩ／Ｏインタフェース１１０はＷＳ本体１００と入力装置（キーボード）および出力装置（ディスプレイ）のインタフェースであり、キーボードからの入力信号の内部バス１６０への転送、内部バス１６０からの信号のディスプレイへの出力等の機能を持つ。尚、本実施例では入力装置をキーボード、出力装置をディスプレイとしたが本構成は本発明を限定するものではない。

【００２３】ＣＰＵ１２０はキーボードから入力する情報、およびＬＡＮインタフェース１４０を介して入力する他端末等からの情報の処理と各機能ブロックの制御を行うブロックである。メモリ１３０は前述の各種情報を格納する機能ブロックであり、ＣＰＵ１２０の処理待ち、ディスプレイへの出力待ち等の場合に当該情報を格納する。ＬＡＮインタフェース１４０はＷＳをネットワーク（ＬＡＮ）に接続するための機能を有するブロック

8

であり、内部バス１６０の伝送フォーマットとＬＡＮの伝送フォーマットの変換を行うと共に、ＭＡＣ(Media Access Control)層の終端、転送情報の暗号化を行う。ＦＤ制御部１５０はＣＰＵ１２０の指示に従って、フロッピーディスク（以下ＦＤ）からのローディング，ＦＤへのセーブ等の機能を持つ。内部バス１６０はＷＳが処理するデータを転送するデータバスと、各機能ブロックを制御するための制御情報を転送する制御情報バスからなる。

【００２４】図３はＬＡＮインタフェース１４０の機能ブロック図である。ＬＡＮインタフェース１４０はバスインタフェース１７０，ＬＡＮ制御部１８０，ＲＯＭ１９０，暗号化部２００，伝送部２１０から構成される。

【００２５】バスインタフェース１７０は内部バス１６０からの情報ブロックの切り出し、情報ブロックのＬＡＮ制御部１８０への転送、更に、ＬＡＮ制御部１８０から転送された情報ブロックのバッファリング、情報ブロックの内部バスへの乗せ換えを行う。ＬＡＮ制御部１８０はパケットの生成／分解，パケットヘッダの付加／削除等のＭＡＣレイヤ機能を実現するブロックである。パケットヘッダには送信端末アドレス（送信元アドレス）と受信端末アドレス（宛先アドレス）が含まれる。送信元アドレスにはＲＯＭ１９０に登録されているＭＡＣアドレスが書き込まれる。ＲＯＭ１９０に登録されているＭＡＣアドレスは、ＷＳだけに割り当てられたアドレスである。一方、宛先アドレスにはパケットの送信先のＷＳに割り当てられたＭＡＣアドレスが書き込まれる。これらの宛先ＷＳのＭＡＣアドレスはデータベースとしてＬＡＮ制御部１８０内のメモリに記憶されている。暗号化部２００はＬＡＮ制御部１８０からの情報の暗号化を行うと共に、ＬＡＮから受信した暗号化情報を解読しＬＡＮ制御部１８０に転送する。伝送部２１０は暗号化部２００からの情報を、接続するＬＡＮの伝送フォーマットに変換しＬＡＮに転送する。また、ＬＡＮから転送される情報を自ＷＳ内のフォーマットに変換する。

【００２６】次に図１を用いて暗号化部２００を詳細に説明する。図１において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵／ＩＤ読み出し回路２１２に転送する。暗号化鍵／ＩＤ読み出し回路２１２はカウント値に基づき、パケットの暗号化に使用する暗号化鍵と暗号化鍵を一意に示す暗号化鍵識別子（以下、暗号化鍵ＩＤと称す）をメモリ２１３より読み出す。

【００２７】図４（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されており、各暗号化鍵に１６進表示で００からＦＦまでの暗号化鍵ＩＤ３０３が登録させている。尚、異なる複数の暗号化鍵ＩＤに対して同一の暗号化鍵を対応させることも可能である。そのような場合に

は、２５６種類のカウント値と暗号化鍵ＩＤに対して２５６種類以下の暗号化鍵が登録される。更に、暗号化鍵／ＩＤ読み出し回路２１２は暗号化鍵を暗号化回路２１５に転送すると共に、暗号化鍵ＩＤを暗号化鍵ＩＤ挿入回路２１６に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化鍵ＩＤ挿入回路２１６はパケットの所定の位置に、暗号化鍵／ＩＤ読み出し回路２１２より転送された暗号化鍵ＩＤを挿入する。

【００２８】図５に本実施例における暗号化鍵ＩＤ５０４の挿入位置を示す。パケット500はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。暗号化鍵ID504 はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、暗号化鍵ＩＤ５０４とユーザ情報５０５を情報領域５０１として取扱うので、暗号化鍵ＩＤ５０４の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００２９】一方、暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、暗号化鍵ＩＤ挿入回路２１６に転送する。本実施例では、暗号化鍵ＩＤはネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００３０】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。暗号化鍵ＩＤ分離回路２１７は受信暗号化パケットから暗号化鍵ＩＤの区間を切り出し、解読鍵読み出し回路２１８に転送する。暗号化鍵ＩＤ以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は暗号化鍵ＩＤに基づき、メモリ２１９より解読鍵を読み出す。暗号化鍵ＩＤは共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵ＩＤを解読することができる。尚、本実施例では暗号化鍵ＩＤの暗号化に共通暗号化鍵を用いているので平文の暗号化鍵ＩＤと暗号化した暗号化鍵ＩＤは一対一に対応するので、受信したパケットの暗号化鍵ＩＤを解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵ＩＤを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は暗号化鍵ＩＤ分離回路２１７が切り出した暗号化鍵ＩＤをそのまま用いて解読鍵を選択する。

【００３１】図４（ｂ）にメモリ２１９の構成例を示す。本実施例では１６進表示で００からＦＦまでの暗号化鍵ＩＤ４０１に対して、一対一に対応するように解読鍵402が２５６種類登録されている。尚、メモリ２１３と同様に異なる複数の暗号化鍵ＩＤに対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類の暗号化鍵ＩＤに対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８は暗号化鍵ＩＤで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００３２】次に本実施例におけるカウント値／暗号化鍵／暗号化鍵ＩＤ／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウント値／暗号化鍵／暗号化鍵ＩＤを登録するメモリ２１３への設定データの書き込み制御はメモリ書込制御２２２が行う。一方、暗号化鍵ＩＤ／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ書込制御２２２およびメモリ書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００３３】次に図６，図７を用いて第二の実施例について説明する。本実施例ではＬＡＮ制御部１８０から入力するパケットの宛先アドレスに基づいて使用する暗号化鍵を決定する。尚、本実施例は第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００３４】図６において、宛先アドレス読み出し回路２２４はＬＡＮ制御部１８０から入力するパケットの宛先アドレスを読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５は宛先アドレスに基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００３５】図７（ａ）に本実施例におけるメモリ２１３の構成例を示す。メモリ２１３では２５６種類の送信パケット宛先アドレス３０４（ＤＡ＃０～ＤＡ＃２５５）に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。宛先アドレスには各端末への個別通信用のアドレスと複数の端末に共通に付与されているグループ通信用のアドレスと、全ての端末に共通に付与されている一斉同報通信用のアドレスがある。尚、異なる複数の宛先アドレスに対して同一の暗号化鍵を対応させることも可能である。そのような場合には２５６種類の宛先アドレスに対して２５６種類以下の暗号化鍵が登録される。更に、宛先アドレスと送信元アドレスの組み合わせに対して、一対一に対応するように暗号化鍵を登録することも可能である。更に、暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗

号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００３６】本実施例では、第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと一致する。

【００３７】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。宛先アドレス分離回路２２６は暗号化パケットから宛先アドレスの区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８は宛先アドレスに基づき、メモリ２１９より解読鍵を読み出す。宛先アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は宛先アドレスを解読することができる。尚、本実施例では宛先アドレスの暗号化に共通暗号化鍵を用いていることから平文の宛先アドレスと暗号化した宛先アドレスは一対一に対応するので、受信したパケットの宛先アドレスを解読せずに用いて解読鍵を選択することも可能である。また、宛先アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は宛先アドレス分離回路２２６が複写した宛先アドレスをそのまま用いて解読鍵を選択する。

【００３８】図７（ｂ）にメモリ２１９の構成例を示す。本実施例では（Ｎ＋２）種類の受信パケットの宛先アドレス４０３に対して（Ｎ＋２）種類の解読鍵４０２が一対一に対応するように登録されている。具体的には、自ＷＳが個別通信の受信端末となる場合の自アドレス１種類、自ＷＳを含むグループに対するグループ通信を行う場合のグループアドレスＮ種類、全ての端末に対する同報通信を行う場合の一斉同報アドレス１種類の計（Ｎ＋２）種類のアドレスに対して、一対一に対応するように（Ｎ＋２）種類の解読鍵４０２が登録されている。尚、異なる複数の受信パケット宛先アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には（Ｎ＋２）種類の宛先アドレスに対して（Ｎ＋２）種類以下の解読鍵が登録される。更には、宛先アドレスと発信元アドレスの組み合わせに対して、一対一に対応するように解読鍵を登録することも可能である。解読鍵読み出し回路２１８は宛先アドレスで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００３９】次に本実施例における送信パケット宛先アドレス／暗号化鍵および受信パケット宛先アドレス／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケット宛先アドレス／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ書込制御２２２が行う。一方、受信パケット宛先アドレス／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ＃２書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ書込制御２２２およびメモリ書込制御２２３に転送される。書込制御２２２，２２３はＣＰＵ１２０の指示に従い、メモリ２１３，メモリ２１９の登録内容の書き換えを行う。

【００４０】次に図８，図９を用いて第三の実施例について説明する。本実施例ではＬＡＮ制御部１８０から入力するパケットのルート情報に基づいて使用する暗号化鍵を決定する。尚、本実施例も前述の第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００４１】図８において、ルート情報読み出し回路２２７はＬＡＮ制御部１８０から入力するパケットのルート情報を読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５はルート情報に基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００４２】図９（ａ）に本実施例におけるメモリ２１３の構成例を示す。メモリ２１３では２５６種類の送信パケットルート情報３０５（ＶＣＮ＃０～ＶＣＮ＃２５５）に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。尚、ルート情報の設定方法は任意であり本発明を制限するものではない。暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は前記暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、ルート情報は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００４３】本実施例でも第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと完全に一致する。

【００４４】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。ルート情報分離回路２２８は暗号化パケットからルート情報の区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８はルート情報に基づき、メモリ２１９より解読鍵を読み出す。ルート情報は共通暗号化鍵で

暗号化されているので、全ての受信端末はルート情報を解読することができる。尚、本実施例ではルート情報の暗号化に共通暗号化鍵を用いているので平文のルート情報と暗号化したルート情報は一対一に対応するので、受信したパケットのルート情報を解読せずに用いて解読鍵を選択することも可能である。また、ルート情報を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合にはルート情報分離回路２２８が複写したルート情報をそのまま用いて解読鍵を選択する。

【００４５】図９（ｂ）にメモリ２１９の構成例を示す。本実施例では受信パケットのルート情報４０４に対して、一対一に対応するように２５６種類の解読鍵４０２が登録されている。尚、異なる複数のルート情報に対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類のルート情報に対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８はルート情報で一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００４６】次に本実施例における送信パケットルート情報／暗号化鍵および受信パケットルート情報／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケットルート情報／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。一方、受信パケットルート情報／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ＃１書込制御２２２およびメモリ＃２書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００４７】次に図１０，図１１を用いて第四の実施例について説明する。本実施例ではパケットを送信する通信端末のＭＡＣアドレスに基づいて使用する暗号化鍵を決定する。従って、物理的に一つの通信端末が複数のＭＡＣアドレスを有する場合には一端末が複数の暗号化鍵を有することになり、複数の通信端末が一つのＭＡＣアドレスを共有する場合には複数の端末が一つの暗号化鍵を共有することになる。尚、本実施例も前述の第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００４８】図１０において、送信元アドレス読み出し回路２２９はＬＡＮ制御部１８０から入力するパケットの送信元アドレスを読み出し、暗号化鍵読み出し回路２２５に転送する。暗号化鍵読み出し回路２２５は前記送信元アドレスに基づき、使用する暗号化鍵をメモリ２１３より読み出す。

【００４９】図１１（ａ）に本実施例におけるメモリ２１３の構成例を示す。本実施例では１種類の送信パケット送信元アドレス３０６に対して一種類の暗号化鍵３０２が登録されている。暗号化鍵読み出し回路２２５は暗号化鍵を暗号化回路２１５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、伝送部２１０に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した暗号化鍵を用いて暗号化する。

【００５０】本実施例でも第一の実施例における暗号化鍵ＩＤのような特有のパラメータを使用しないので、暗号化部２００と伝送部２１０の間で授受するパケットフォーマットはＬＡＮ制御部がサポートするＭＡＣ層プロトコルのパケットフォーマットと一致する。

【００５１】次に、ＬＡＮから暗号化情報（パケット）を受信したときの処理について説明する。送信元アドレス分離回路２３０は暗号化パケットから送信元アドレスの区間を複写し、解読鍵読み出し回路２１８に転送する。解読鍵読み出し回路２１８は送信元アドレスに基づき、メモリ２１９より解読鍵を読み出す。送信元アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は送信元アドレスを解読することができる。尚、本実施例では送信元アドレスの暗号化に共通暗号化鍵を用いていることから平文の送信元アドレスと暗号化した送信元アドレスは一対一に対応するので、受信したパケットの送信元アドレスを解読せずに用いて解読鍵を選択することも可能である。また、送信元アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には送信元アドレス分離回路２３０が複写した送信元アドレスをそのまま用いて解読鍵を選択する。

【００５２】図１１（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の受信パケットの送信元アドレス４０５に対して２５６種類の解読鍵４０２が一対一に対応するように登録されている。尚、異なる複数の受信パケット送信元アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には２５６種類の宛先アドレスに対して２５６種類以下の解読鍵が登録される。解読鍵読み出し回路２１８は送信元アドレスで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１はバッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００５３】次に本実施例における送信パケット送信元

アドレス／暗号化鍵および受信パケット送信元アドレス／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、ＦＤより設定データをロードする。送信パケット送信元アドレス／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３書込制御２２２が行う。一方、受信パケット送信元アドレス／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２およびメモリ２１９の書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００５４】次に図１２，図１３および１４を用いて第五の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は暗号化鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００５５】図１２において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵読み出し回路２３１に転送する。暗号化鍵読み出し回路２３１はカウント値に基づき、パケットの暗号化に使用する暗号化鍵をメモリ２１３より読み出す。

【００５６】図１３（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２が２５６種類登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵を対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６種類以下の暗号化鍵が登録される。更に、暗号化鍵読み出し回路２３１は暗号化鍵を暗号化回路２１５と暗号化鍵挿入回路２３２に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。暗号化鍵挿入回路２３２はパケットの所定の位置に、暗号化鍵読み出し回路２３１より転送された暗号化鍵を挿入する。

【００５７】図１４に本実施例における暗号化鍵５０６の挿入位置を示す。パケット５００はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。暗号化鍵５０６はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、暗号化鍵５０６とユーザ情報５０５を情報領域５０１として取扱うので、暗号化鍵５０６の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００５８】一方、暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、暗号化鍵挿入回路２３２に転送する。本実施例では、暗号化鍵はネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００５９】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。暗号化鍵分離回路２３３は受信暗号化パケットから暗号化鍵の区間を切り出し、解読鍵読み出し回路２１８に転送する。暗号化鍵以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は暗号化鍵に基づき、メモリ２１９より解読鍵を読み出す。暗号化鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵を解読することができる。尚、本実施例では暗号化鍵の暗号化に共通暗号化鍵を用いていることから平文の暗号化鍵と暗号化した暗号化鍵は一対一に対応するので、受信したパケットの暗号化鍵を解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には暗号化鍵分離回路２３３が切り出した暗号化鍵をそのまま用いて解読鍵の選択を行う。

【００６０】図１３（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の暗号化鍵４０６（Ｃ－Ｋｅｙ＃０～Ｃ－Ｋｅｙ＃２５５）に一対一に対応するように解読鍵４０２（Ｄ－Ｋｅｙ＃０～Ｄ－Ｋｅｙ＃２５５）が２５６種類登録されている。解読鍵読み出し回路２１８は暗号化鍵で一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００６１】次に本実施例におけるカウント値／暗号化鍵／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク（ＦＤ）より設定データをロードする。カウント値／暗号化鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ＃１書込制御２２２が行う。一方、暗号化鍵／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２およびメモリ219の書込制御２２３に転送される。書込制御２２２および２２３はＣＰＵ１２０の指示に基づき、メモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００６２】次に図１５，図１６および図１７を用いて第六の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は解読鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００６３】図１５において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵／解読鍵読み出し回路２３４に転送する。暗号化鍵／解読鍵読み出し回路２３４はカウント値に基づき、パケットの暗号化に使用する暗号化鍵および解読時に使用する解読鍵をメモリ２１３より読み出す。

【００６４】図１６にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２と解読鍵３０７が２５６組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵／解読鍵を対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６組以下の暗号化鍵／解読鍵が登録される。更に、暗号化鍵／解読鍵読み出し回路２３４は暗号化鍵を暗号化回路２１５に転送すると共に、解読鍵を解読鍵挿入回路２３５に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。解読鍵挿入回路２３２はパケットの所定の位置に、暗号化鍵／解読鍵読み出し回路２３４より転送された解読鍵を挿入する。

【００６５】図１７に本実施例における解読鍵５０７の挿入位置を示す。パケット５００はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。解読鍵５０７はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、解読鍵５０７とユーザ情報５０５を情報領域５０１として取扱うので、解読鍵５０７の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００６６】暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、解読鍵挿入回路２３５に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００６７】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。解読鍵分離回路２３６は受信暗号化パケットから解読鍵の区間を切り出し、解読回路２２１に転送する。解読鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵を解読することができる。また、解読鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵分離回路２３６が切り出した解読鍵をそのまま用いる。解読回路２２１は解読鍵分離回路２３６より転送されるパケットを当該解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００６８】次に本実施例におけるカウント値／暗号化鍵／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク（ＦＤ）より設定データをロードする。カウント値／暗号化鍵／解読鍵を登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のＣＰＵ１２０で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２に転送される。書込制御２２２はCPU120の指示に基づきメモリ２１３の登録内容の書き換えを行う。

【００６９】次に図１８，図１９および２０を用いて第七の実施例について説明する。第一の実施例が暗号化鍵ＩＤを暗号化情報と共に転送するのに対して、本実施例は解読鍵識別子（以下、解読鍵ＩＤと称す）を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部２００の動作のみが異なるので、暗号化部２００のみ説明する。

【００７０】図１８において、入力パケットカウント回路２１１はＬＡＮ制御部１８０から入力するパケット数をカウントし、カウント値を暗号化鍵／ＩＤ読み出し回路２１２に転送する。暗号化鍵／ＩＤ読み出し回路２１２はカウント値に基づき、パケットの暗号化に使用する暗号化鍵と暗号化鍵に対応する解読鍵を一意に示す解読鍵ＩＤをメモリ２１３より読み出す。

【００７１】図１９（ａ）にメモリ２１３の構成例を示す。本実施例では０から２５５までのカウント値３０１に対して、一対一に対応するように暗号化鍵３０２と解読鍵ＩＤ３０８が２５６組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵／解読鍵ＩＤを対応させることも可能である。そのような場合には２５６種類のカウント値に対して２５６組以下の暗号化鍵／解読鍵ＩＤが登録される。更に、暗号化鍵／解読鍵読み出し回路２１２は暗号化鍵を暗号化回路215に転送すると共に、解読鍵ＩＤを解読鍵ＩＤ挿入回路２３７に転送する。バッファ２１４は暗号化鍵の転送までの時間だけＬＡＮ制御部１８０から入力したパケットを格納する。解読鍵ＩＤ挿入回路２３７はパケットの所定の位置に、暗号化鍵／ＩＤ読み出し回路２１２より転送された解読鍵ＩＤを挿入する。

【００７２】図２０に本実施例における解読鍵ＩＤ５０８の挿入位置を示す。パケット500はパケットヘッダと情報領域５０１から構成される。パケットヘッダ内には宛先アドレス５０２と送信元アドレス５０３が書き込まれている。解読鍵ＩＤ５０８はユーザ情報５０５とパケットヘッダの間に挿入する。ＭＡＣ層では、解読鍵ＩＤ

５０８とユーザ情報５０５を情報領域５０１として取扱うので、解読鍵ＩＤ５０８の挿入はＭＡＣ層プロトコルには影響を及ぼさない。

【００７３】暗号化回路２１５はバッファ２１４より入力するパケットを暗号化し、解読鍵ＩＤ挿入回路２３７に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ２１３より読み出した個別の暗号化鍵を用いて暗号化する。

【００７４】次に、ＬＡＮから暗号化情報を受信したときの処理について説明する。解読鍵ＩＤ分離回路２３７は受信暗号化パケットから解読鍵ＩＤの区間を切り出し、解読鍵読み出し回路２１８に転送する。解読鍵ＩＤ以外の部分はそのままバッファ２２０に格納される。解読鍵読み出し回路２１８は前記解読鍵ＩＤに基づき、メモリ２１９より解読鍵を読み出す。解読鍵ＩＤは共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵ＩＤを解読することができる。尚、本実施例では解読鍵ＩＤの暗号化に共通暗号化鍵を用いていることから平文の解読鍵ＩＤと暗号化した解読鍵ＩＤは一対一に対応するので、受信したパケットの解読鍵ＩＤを解読せずに用いて解読鍵を選択することも可能である。また、解読鍵ＩＤを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵ＩＤ分離回路２３８が切り出した解読鍵ＩＤをそのまま用いて解読鍵の選択を行う。

【００７５】図１９（ｂ）にメモリ２１９の構成例を示す。本実施例では２５６種類の解読鍵ＩＤ４０７に一対一に対応するように解読鍵４０２が２５６種類登録されている。解読鍵読み出し回路２１８は解読鍵ＩＤで一意に定まる解読鍵を読み出し、解読回路２２１に転送する。解読回路２２１は、バッファ２２０より入力するパケットを解読鍵を用いて解読し、ＬＡＮ制御部１８０に転送する。

【００７６】次に本実施例におけるカウント値／暗号化鍵／解読鍵ＩＤ／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(ＦＤ)より設定データをロードする。カウント値／暗号化鍵／解読鍵ＩＤを登録するメモリ２１３への設定データの書き込み制御はメモリ２１３の書込制御２２２が行う。解読鍵ＩＤ／解読鍵を登録するメモリ２１９への設定データの書き込み制御はメモリ２１９の書込制御２２３が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、ＷＳ本体１００内のCPU120で処理された設定データが内部バス１６０を介してメモリ２１３の書込制御２２２に転送される。書込制御２２２はＣＰＵ１２０の指示に基づきメモリ２１３およびメモリ２１９の登録内容の書き換えを行う。

【００７７】次に図２１，図２２を用いて第八の実施例について説明する。第七の実施例は第一の実施例とメモリ２１３，メモリ２１９の設定方法が異なる。即ち、第一の実施例ではメモリ２１３，２１９の設定はＦＤより設定データをローディングすることにより行った。本実施例では、図２１に示すようにメモリ２１３，２１９の設定データはＬＡＮインタフェース１４０内のＲＯＭ１９１から読み込む。

【００７８】図２２において、書込制御２３９はＲＯＭ１９１よりメモリ２１３への設定データ（カウント値／暗号化鍵／暗号化鍵ＩＤ）を読み込み、メモリ２１３に書き込む。書込制御２４０はＲＯＭ１９１よりメモリ２１９への設定データ（暗号化鍵ＩＤ／解読鍵）を読み込み、メモリ２１９に書き込む。

【００７９】尚、本実施例を前記第二ないし第七の実施例に適用することは容易である。第二の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケット宛先アドレス／暗号化鍵とし、メモリ２１９用として受信パケット宛先アドレス／解読鍵とすれば良い。第三の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケットルート情報／暗号化鍵とし、メモリ２１９用として受信パケットルート情報／解読鍵とすれば良い。第四の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用として送信パケット送信元アドレス／暗号化鍵、メモリ２１９用として受信パケット送信元アドレス／解読鍵とすれば良い。第五の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵、メモリ２１９用として暗号化鍵／解読鍵とすれば良い。第六の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵／解読鍵とすれば良い。第七の実施例に適用する場合には、ＲＯＭ１９１に記憶する内容を、メモリ２１３用としてカウント値／暗号化鍵／解読鍵ＩＤ、メモリ２１９用として解読鍵ＩＤ／解読鍵とすれば良い。

【００８０】

【発明の効果】本発明によれば、暗号化情報と共に暗号化鍵／解読鍵を一意に示す識別情報を転送するので、複数の暗号化鍵を用いる秘匿通信においても暗号化情報を正確に解読することができる。

【００８１】識別情報として暗号化鍵あるいは解読鍵そのものを用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来るので、秘匿通信の信頼性がより向上する。

【００８２】識別情報として暗号化鍵識別子あるいは解読鍵識別子を用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来ることに加えて、暗号化鍵あるいは解読鍵を識別子として表現しているので、更に秘匿通信の信頼性が向上する。

【００８３】識別情報として端末アドレスあるいはルー

21

ト情報を用いる場合には、特別な識別子を使用することなく暗号化鍵／解読鍵を特定することが出来る。

【図面の簡単な説明】

【図１】本発明の第一の実施例における暗号化部のブロック図。

【図２】本発明の第一の実施例における通信端末（ＷＳ）本体のブロック図。

【図３】本発明の第一の実施例におけるＬＡＮインタフェースのブロック図。

【図４】本発明の第一の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図５】本発明の第一の実施例におけるパケットの説明図。

【図６】本発明の第二の実施例における暗号化部のブロック図。

【図７】本発明の第二の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図８】本発明の第三の実施例における暗号化部のブロック図。

【図９】本発明の第三の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１０】本発明の第四の実施例における暗号化部のブロック図。

【図１１】本発明の第四の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１２】本発明の第五の実施例における暗号化部のブロック図。

22

【図１３】本発明の第五の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図１４】本発明の第五の実施例におけるパケットの説明図。

【図１５】本発明の第六の実施例における暗号化部のブロック図。

【図１６】本発明の第六の実施例における暗号化鍵および解読鍵記憶部の説明図。

【図１７】本発明の第六の実施例におけるパケットの説明図。

【図１８】本発明の第七の実施例における暗号化部のブロック図。

【図１９】本発明の第七の実施例における暗号化鍵記憶部および解読鍵記憶部の構成図。

【図２０】本発明の第七の実施例におけるパケットの説明図。

【図２１】本発明の第八の実施例におけるＬＡＮインタフェースのブロック図。

【図２２】本発明の第八の実施例における暗号化部のブロック図。

【符号の説明】

２００…暗号化部、２１１…入力パケットカウント回路、２１２…暗号化鍵／ＩＤ読み出し回路、２１３…メモリ、２１５…暗号化回路、２１６…暗号化鍵ＩＤ挿入回路、２１７…暗号化鍵ＩＤ分離回路、２１８…解読鍵読み出し回路、２１９…メモリ、２２１…解読回路、２２２…メモリ書込制御、２２３…メモリ書込制御。

【図9】

図９

(a)

305 送信パケットルート情報	303 暗号化鍵
VCN#0	C-Key#0
VCN#1	C-Key#1
⋮	⋮
VCN#254	C-Key#254
VCN#255	C-Key#255

(b)

404 受信パケットルート情報	402 解読鍵
VCN#0	D-Key#0
VCN#1	D-Key#1
⋮	⋮
VCN#254	D-Key#254
VCN#255	D-Key#255

【図１１】

図１１

(a)

306 送信パケット送信元アドレス	302 解読鍵
SA#0	C-Key#0

(b)

405 受信パケット送信元アドレス	402 解読鍵
SA#0	D-Key#0
SA#1	D-Key#1
⋮	⋮
SA#254	D-Key#254
SA#255	D-Key#255

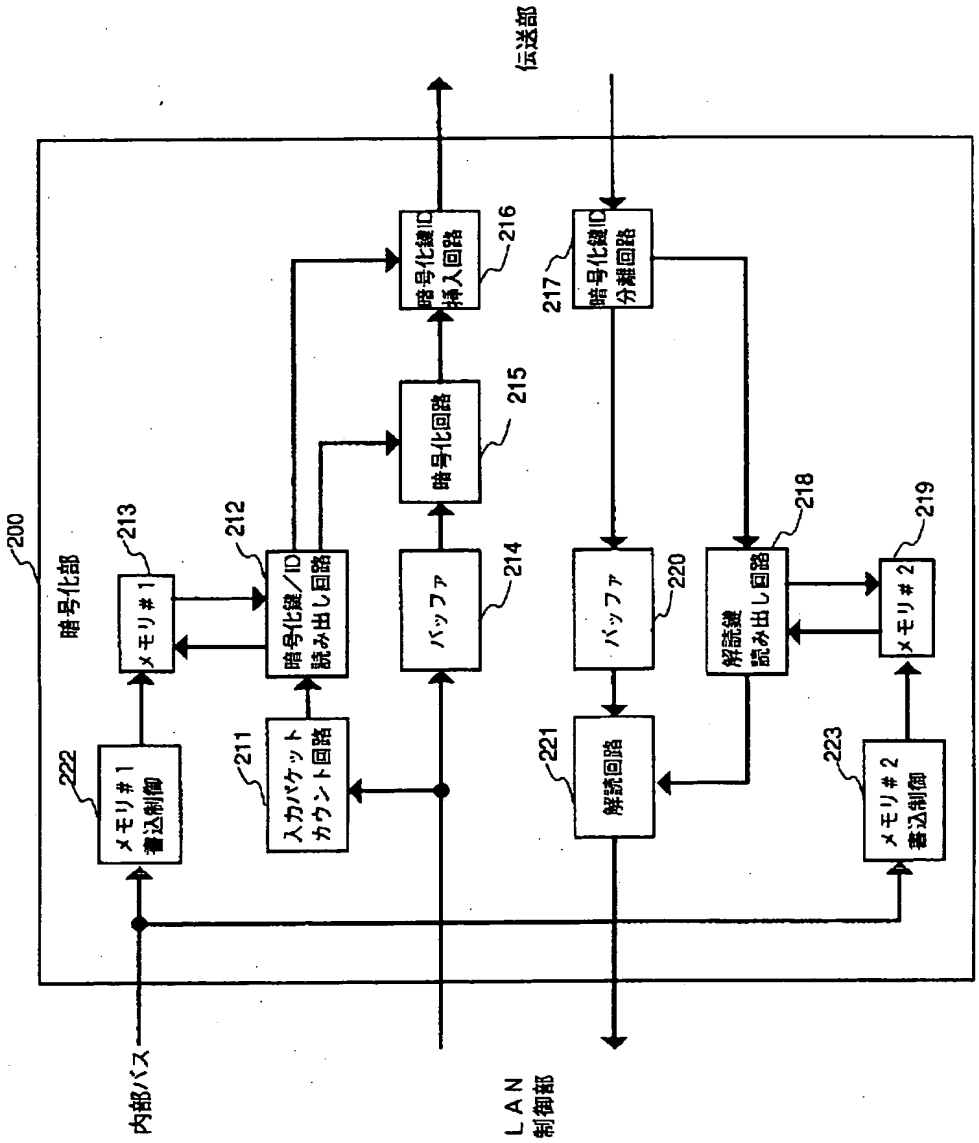
【図１６】

図１６

301 カウント値	302 暗号化鍵	307 解読鍵
0	C-Key#0	D-Key#0
1	C-Key#1	D-Key#1
⋮	⋮	⋮
254	C-Key#254	D-Key#254
255	C-Key#255	D-Key#255

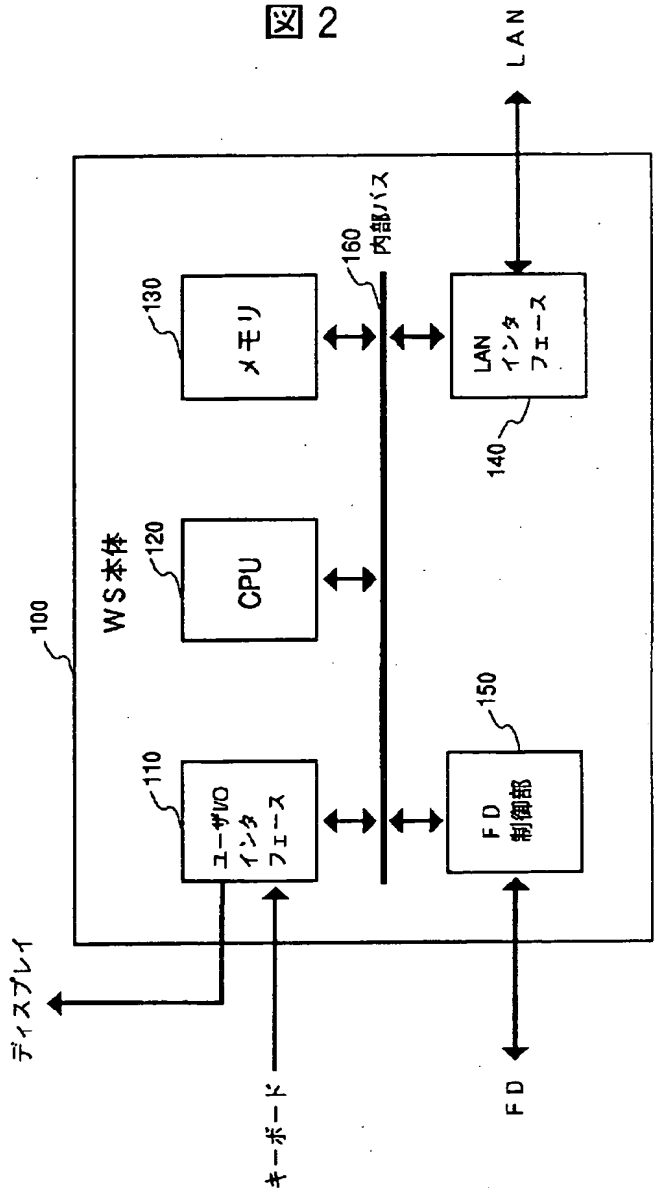
【図１】

図１


伝送部
200
暗号化部
213
メモリ＃１
212
暗号化鍵／ID読み出し回路
暗号化鍵ID挿入回路
216
暗号化回路
215
バッファ
214
222
メモリ＃１書込制御
211
入力パケットカウント回路
内部バス
LAN制御部
217
暗号化鍵ID分離回路
バッファ
220
221
解読回路
218
解読鍵読み出し回路
219
メモリ＃２
223
メモリ＃２書込制御

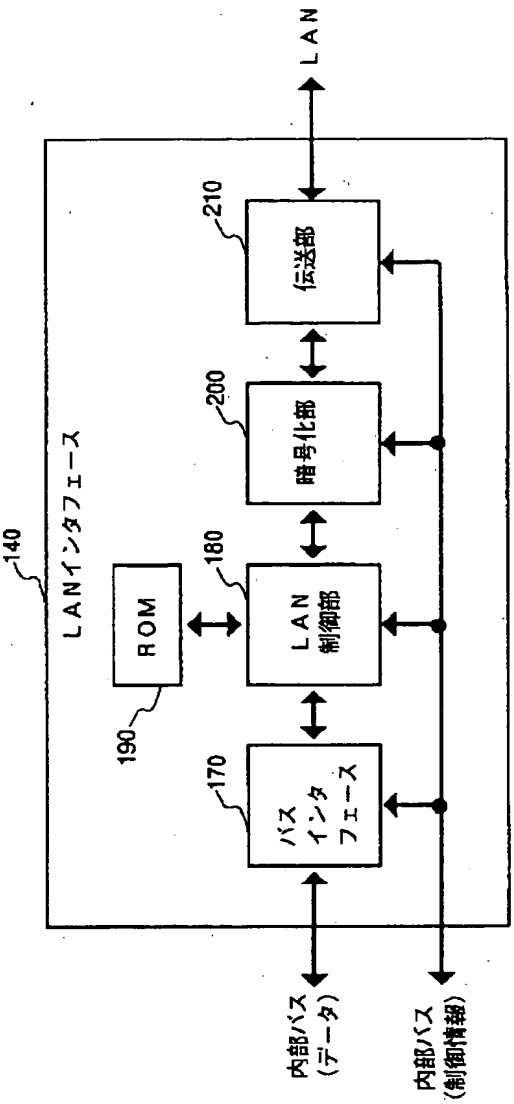
【図2】

図2


LAN
160 内部バス
130 メモリ
LAN インタフェース
140
WS本体
120 CPU
100
110 ユーザI/O インタフェース
150 FD 制御部
ディスプレイ
キーボード
FD

【図3】

図3


LAN
210 伝送部
200 暗号化部
180 LAN 制御部
140 LANインタフェース
ROM
190
170 バス インタフェース
内部バス (データ)
内部バス (制御情報)

【図4】

図4

(a)

301 カウント値	302 暗号化鍵	303 暗号化鍵ID(H)
0	C-Key#0	00
1	C-Key#1	01
⋮	⋮	⋮
254	C-Key#254	FE
255	C-Key#255	FF

(b)

401 暗号化鍵ID(H)	402 解読鍵
00	D-Key#0
01	D-Key#1
⋮	⋮
FE	D-Key#254
FF	D-Key#255

【図7】

図7

(a)

304 送信パケット宛先アドレス	303 暗号化鍵
DA#0	C-Key#0
DA#1	C-Key#1
⋮	⋮
DA#254	C-Key#254
DA#255	C-Key#255

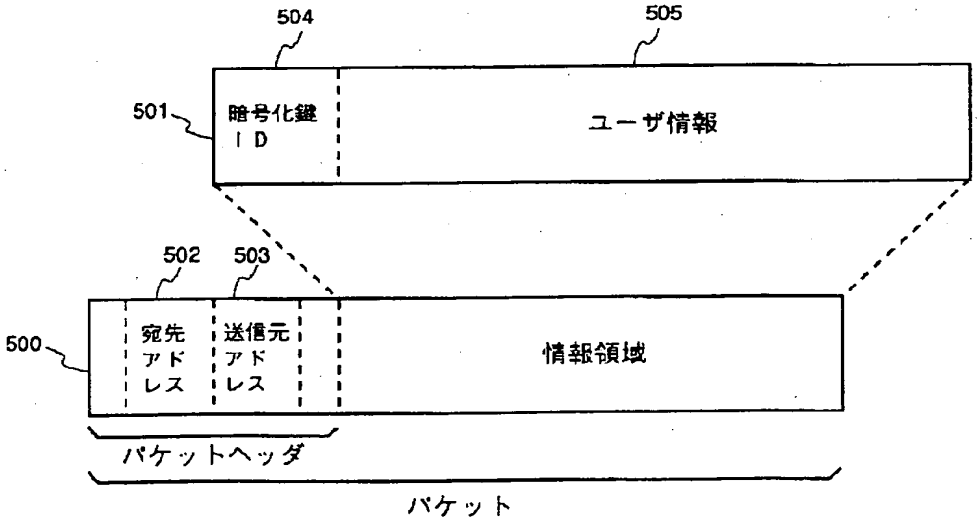
(b)

403 受信パケット宛先アドレス	402 解読鍵
自アドレス	D-Key#X_1
グループアドレス#1	D-Key#X_2
⋮	⋮
グループアドレス#N	D-Key#X_{N+1}
一斉同報アドレス	D-Key#X_{N+2}

但し、$0 \leq X_i \leq 255$ $(1 \leq i \leq N+2)$

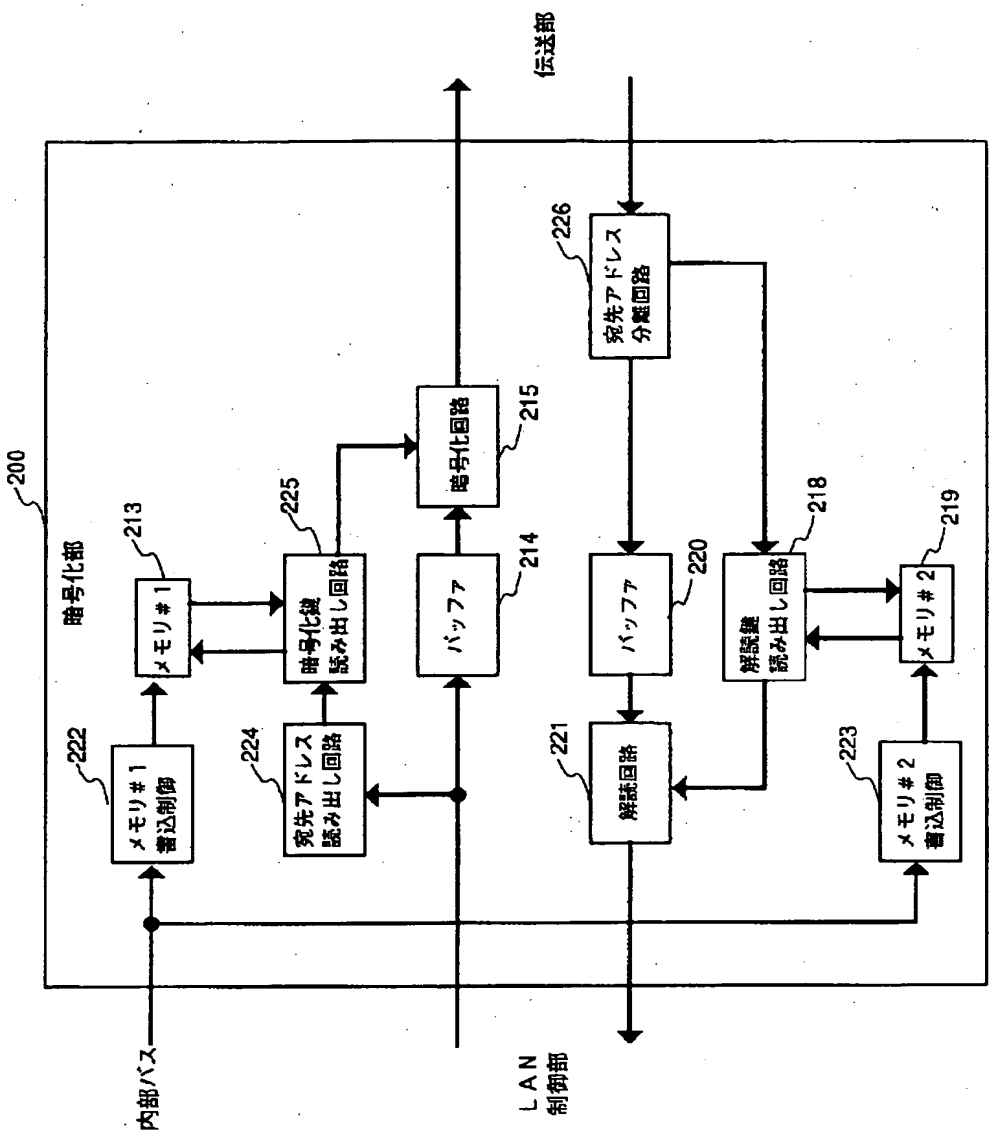
【図5】

図5



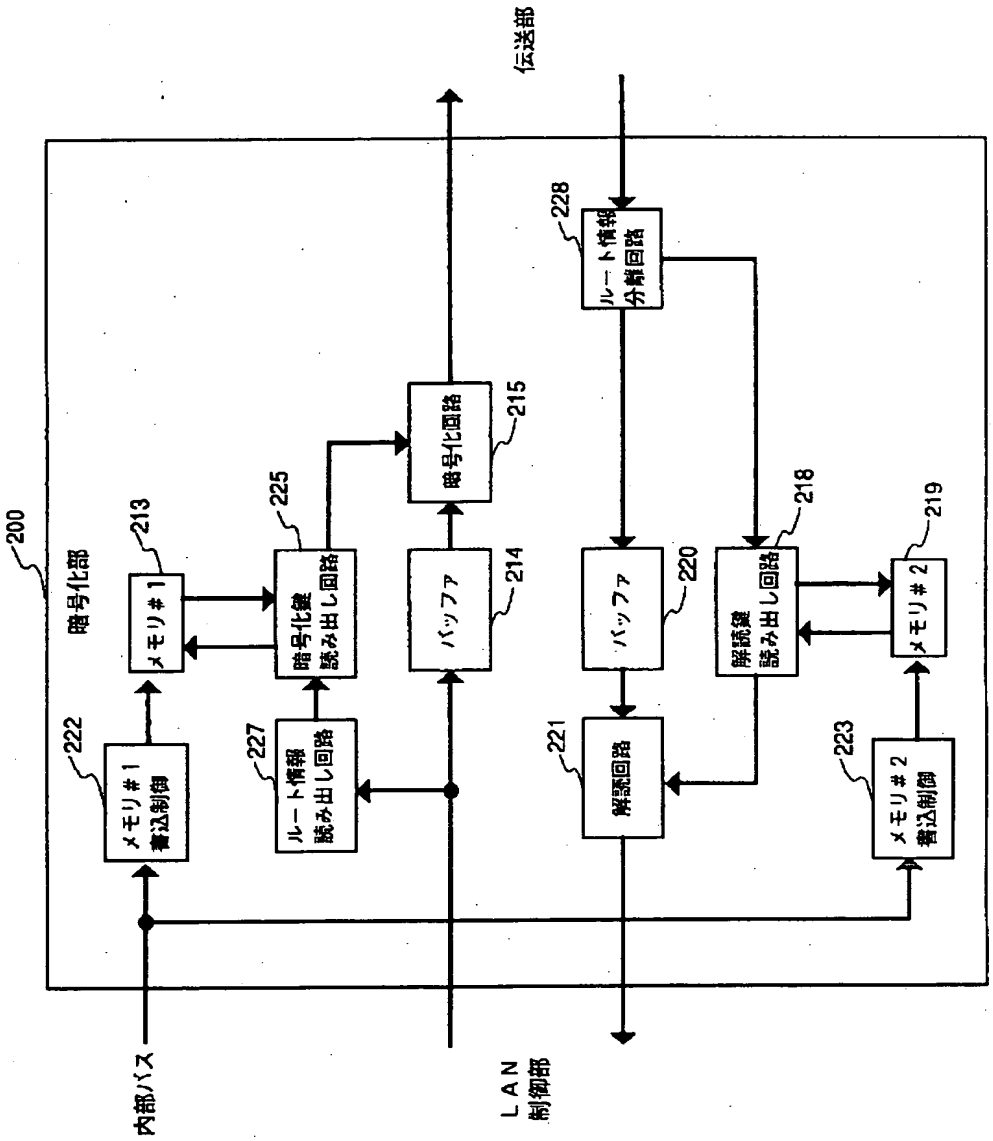
【図６】

図 6


伝送部
200
暗号化部
213
メモリ＃1
225
暗号化鍵
読み出し回路
215
暗号化回路
214
バッファ
226
宛先アドレス
分離回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ＃2
222
メモリ＃1
書込制御
224
宛先アドレス
読み出し回路
221
解読回路
223
メモリ＃2
書込制御
内部バス
LAN
制御部

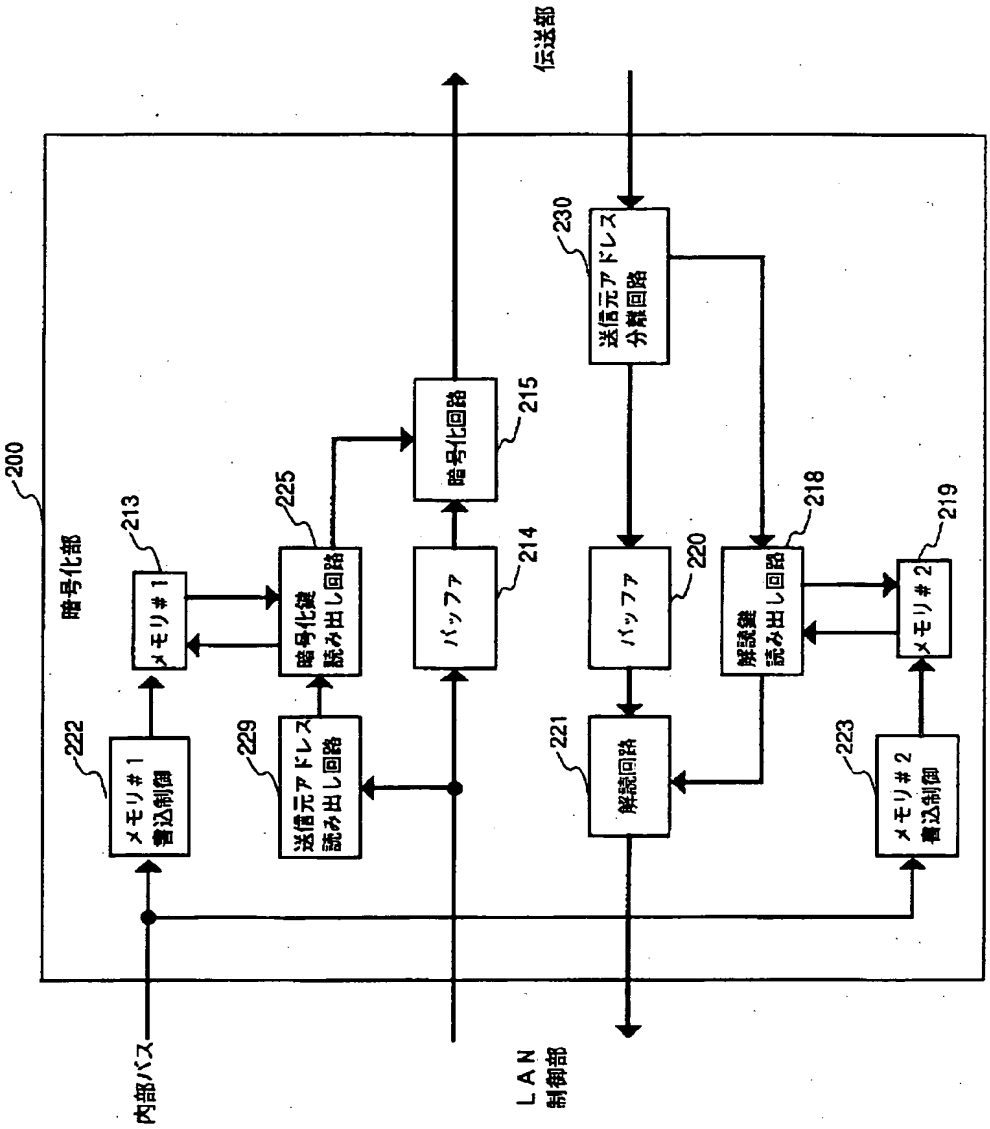
【図８】

図８


伝送部
200
暗号化部
213
メモリ＃１
225
暗号化鍵
読み出し回路
215
暗号化回路
214
バッファ
228
ルート情報
分解回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ＃２
222
メモリ＃１
書込制御
227
ルート情報
読み出し回路
221
解読回路
223
メモリ＃２
書込制御
内部バス
LAN
制御部

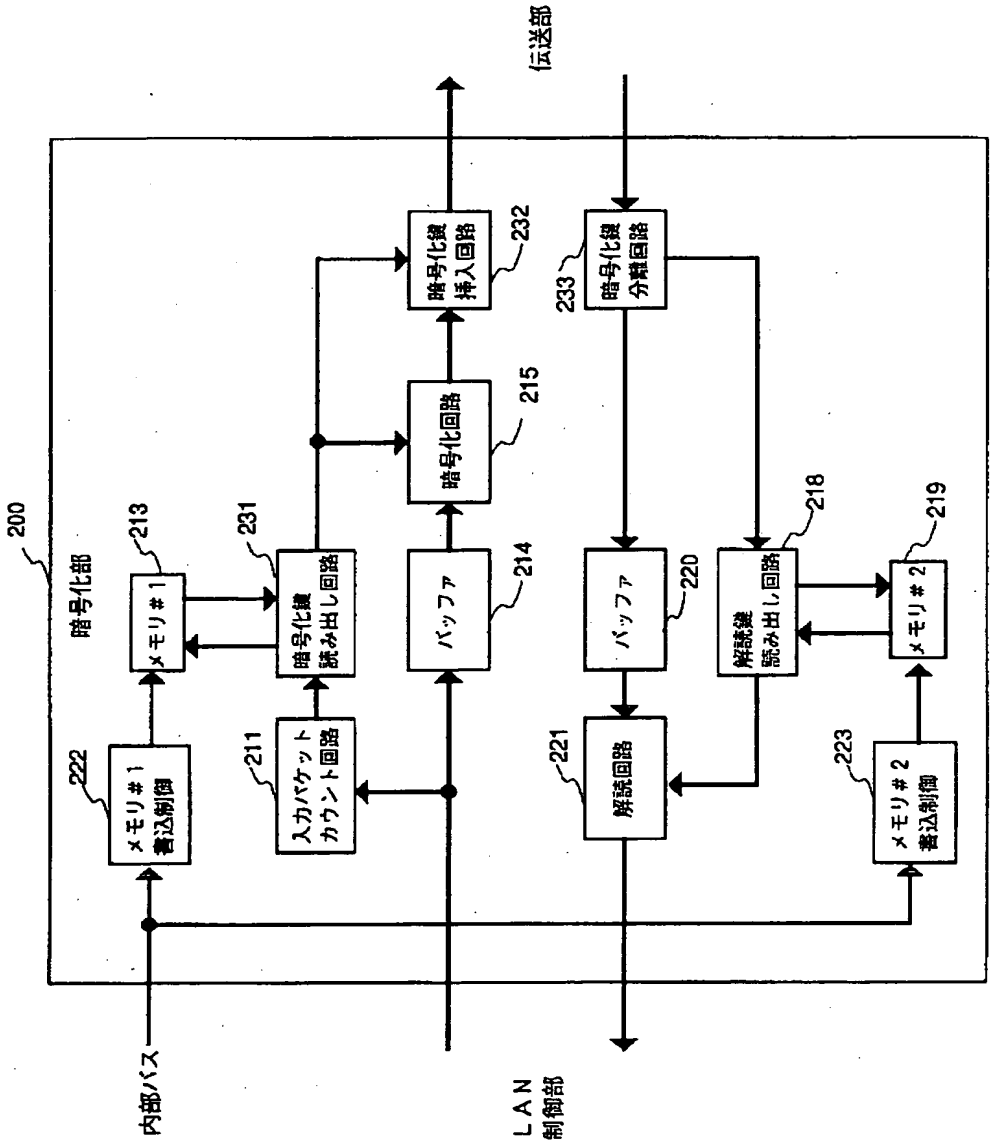
【図10】

図10


伝送部
200
暗号化部
213
メモリ#1
225
暗号化鍵
読み出し回路
215
暗号化回路
214
バッファ
230
送信元アドレス
分離回路
220
バッファ
218
解読鍵
読み出し回路
219
メモリ#2
222
メモリ#1
書込制御
229
送信元アドレス
読み出し回路
221
解読回路
223
メモリ#2
書込制御
内部バス
LAN
制御部

【図１２】

図１２


伝送部
200
暗号化部
213
メモリ＃１
231
暗号化鍵
読み出し回路
暗号化回路
215
暗号化鍵
挿入回路
232
233
暗号化鍵
分離回路
バッファ
214
バッファ
220
218
解読鍵
読み出し回路
219
メモリ＃２
222
メモリ＃１
書込制御
211
入力パケット
カウント回路
221
解読回路
223
メモリ＃２
書込制御
内部バス
ＬＡＮ
制御部

【図１３】

図１３

(a)

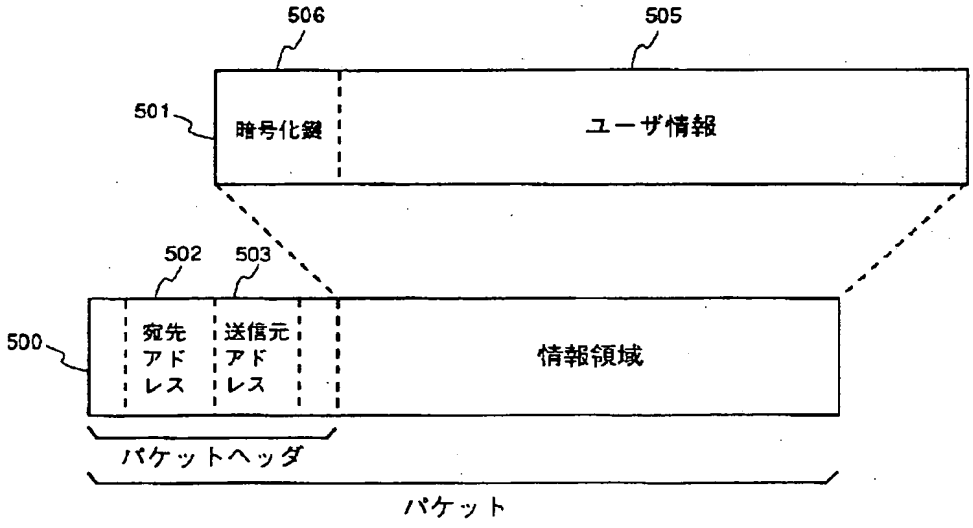
301 カウント値	302 暗号化鍵
0	C-Key#0
1	C-Key#1
⋮	⋮
254	C-Key#254
255	C-Key#255

(b)

406 暗号化鍵	402 解読鍵
C-Key#0	D-Key#0
C-Key#1	D-Key#1
⋮	⋮
C-Key#254	D-Key#254
C-Key#255	D-Key#255

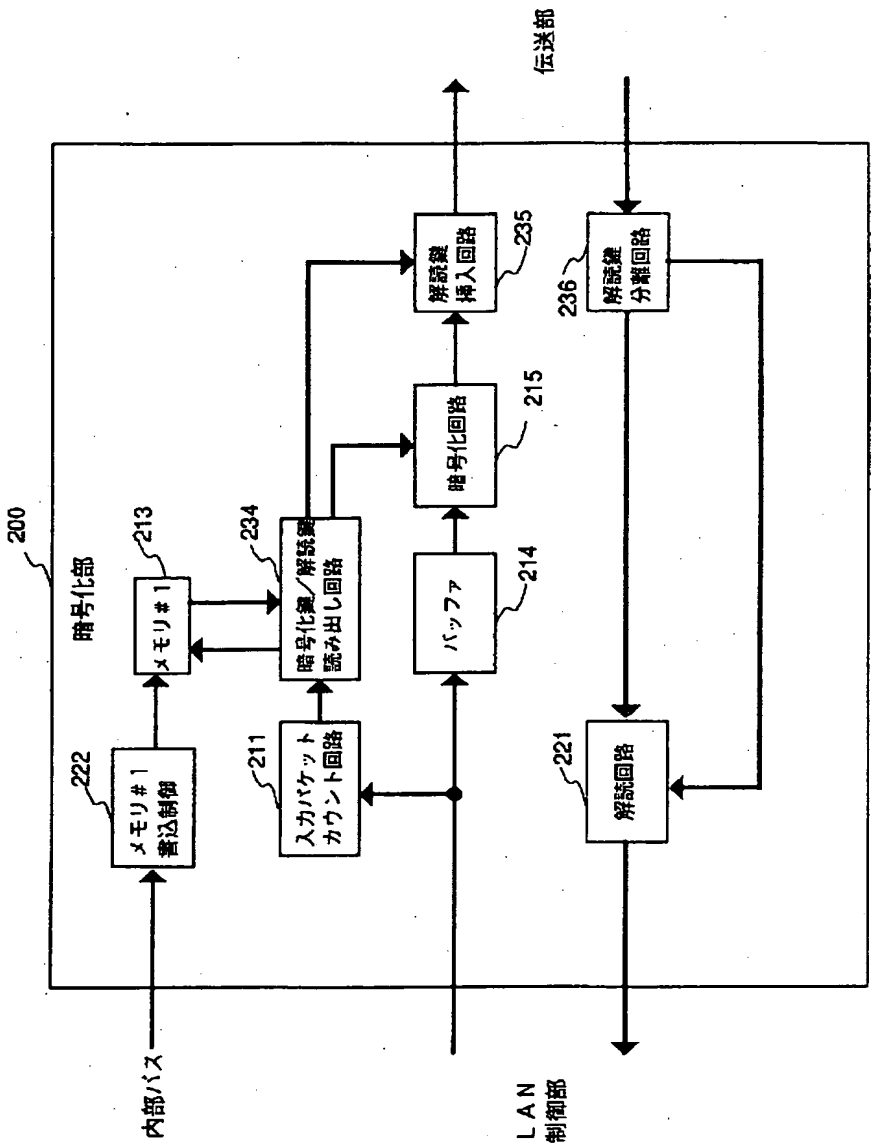
【図１４】

図１４



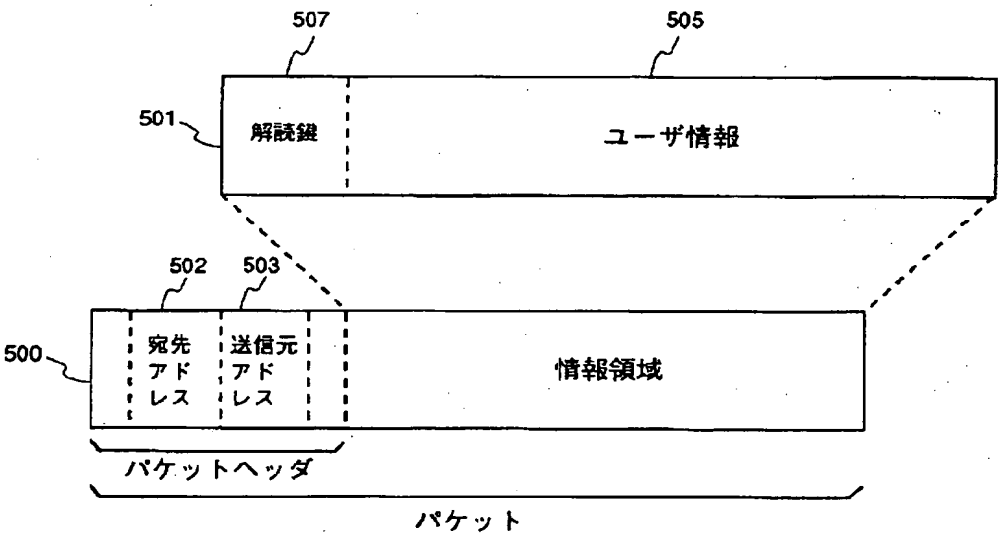
【図１５】

図１５


伝送部
200
暗号化部
213
メモリ＃１
234
暗号化鍵／解読鍵
読み出し回路
235
解読鍵
挿入回路
236
解読鍵
分離回路
215
暗号化回路
214
バッファ
222
メモリ＃１
書込制御
211
入力パケット
カウント回路
221
解読回路
内部バス
LAN
制御部

【図１７】

図１７



【図１９】

図１９

(a)

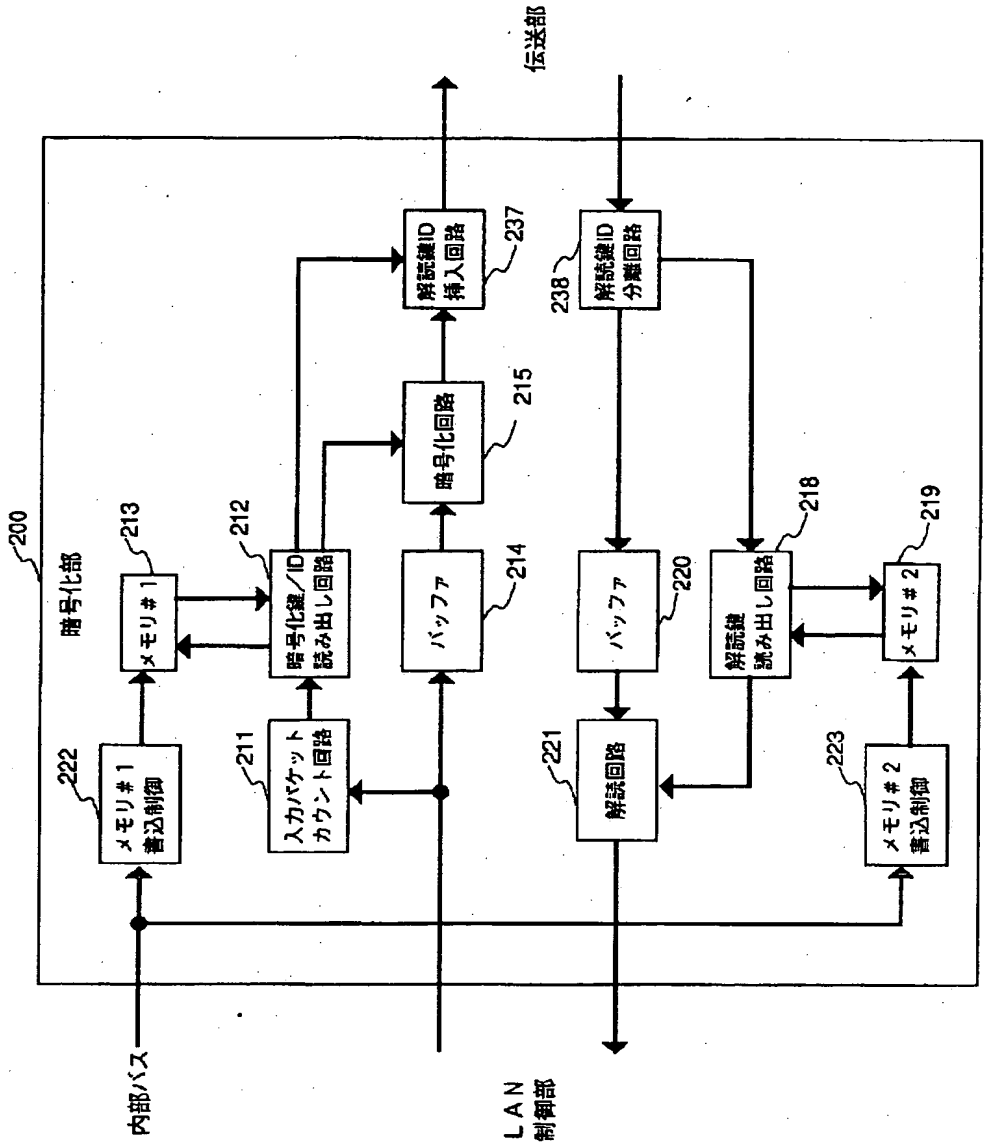
301 カウント値	302 暗号化鍵	303 解読鍵ＩＤ（Ｈ）
0	C-Key#0	00
1	C-Key#1	01
⋮	⋮	⋮
254	C-Key#254	FE
255	C-Key#255	FF

(b)

407 解読鍵ＩＤ（Ｈ）	402 解読鍵
00	D-Key#0
01	D-Key#1
⋮	⋮
FE	D-Key#254
FF	D-Key#255

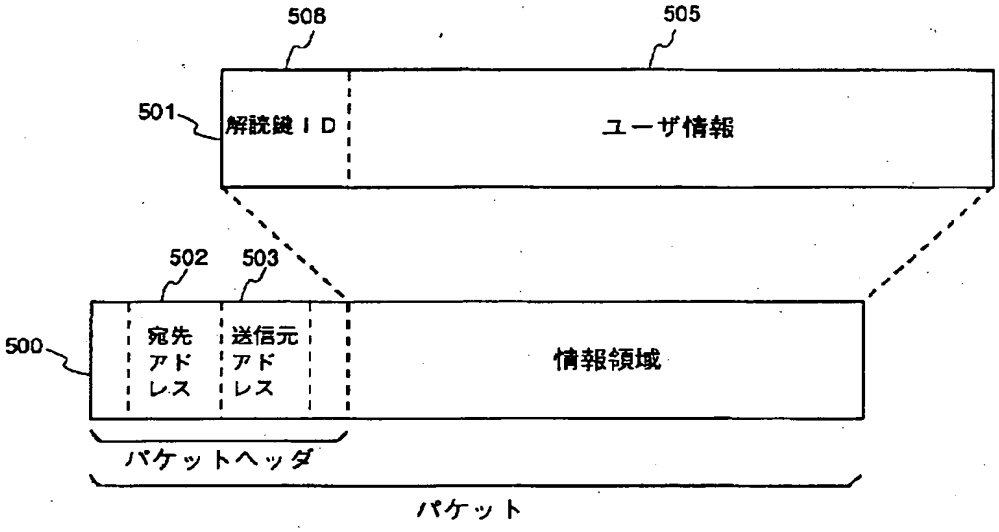
【図１８】

図１８


伝送部
200
暗号化部
213
メモリ＃１
212
暗号化鍵／ID読み出し回路
237
解読鍵ID挿入回路
215
暗号化回路
214
バッファ
238
解読鍵ID分離回路
220
バッファ
218
解読鍵読み出し回路
219
メモリ＃２
222
メモリ＃１書込制御
211
入力パケットカウント回路
221
解読回路
223
メモリ＃２書込制御
内部バス
LAN制御部

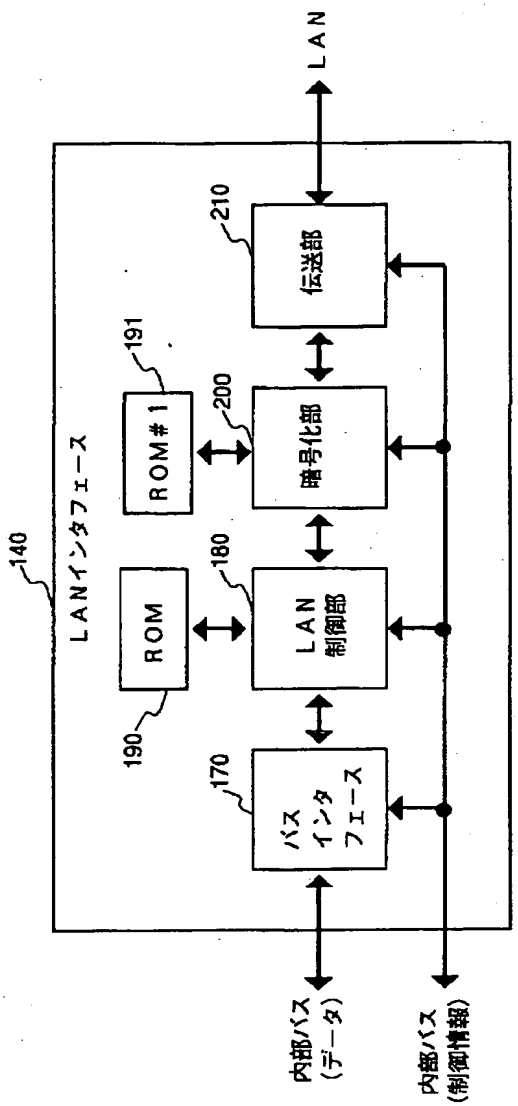
【図２０】

図２０


508
505
501
解読鍵ＩＤ
ユーザ情報
502
503
500
宛先アドレス
送信元アドレス
情報領域
パケットヘッダ
パケット

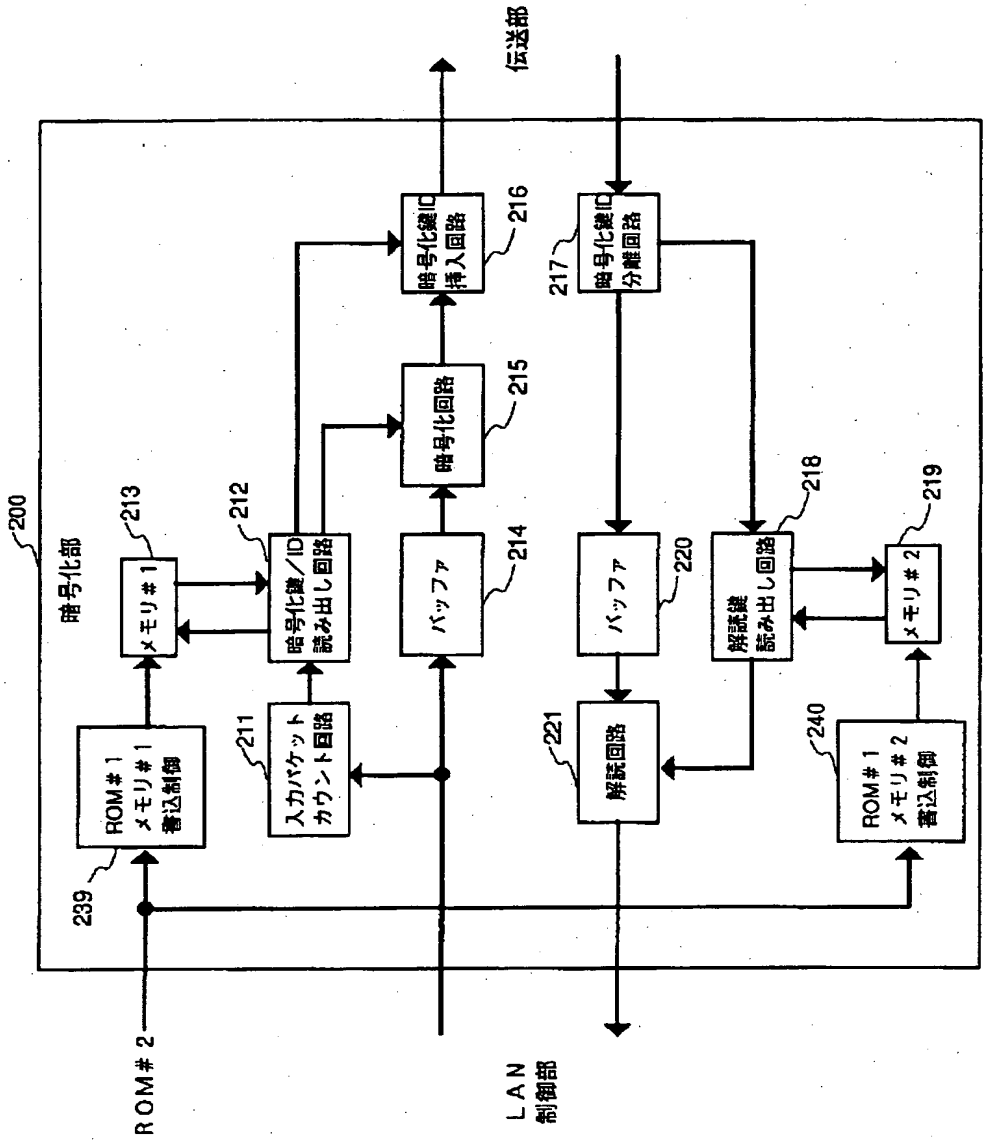
【図２１】

図２１


LAN
210
伝送部
191
ROM#1
200
暗号化部
140
LANインタフェース
ROM
180
LAN制御部
190
170
バスインタフェース
内部バス（データ）
内部バス（制御情報）

【図２２】

図２２



フロントページの続き

(51)Int.Cl.⁵	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　12/28				

(72)発明者　鈴木　秀哉
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内